HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

04/12/2023. Lecture 12.

1 Another construction of a one-way function

Let us consider a function

$$F \; : \; [x,n] \mapsto [x^2 \mod n, n]$$

that transforms a pair of numbers (x, n) in another pair, where the first component is the square of x modulo n, and does not change the second one. It is believed that this function is a *weak one-way function*. It is known that F is easy to reverse in the special case of when n is a prime number (though we did not prove this fact in the class). However, it is believed to be hard to reverse it in case when n is a product of two prime numbers. In fact, the problem of inversion $x^2 \mod n$ for $n = p \cdot q$ (where p and q are prime numbers) is equivalent to factorisation of n. In the class we proved the following statement.

Proposition 1. *Assume there exists a polynomial time algorithm $\mathcal{A}$ (deterministic or randomized) that can invert the function*

$$[x,n] \mapsto [x^2 \mod n, n]$$

for all n that are products of two prime numbers. Then there exists a polynomial time (randomized) algorithm $\mathcal{B}$ that finds prime factors of natural numbers n that are product of two primes.

2 Quadratic residues

An integer number v is called *quadratic residue* modulo n, if there exists an integer number w such that $v = w^2 \mod n$. If $n > 2$ is a prime number, then exactly half of the numbers in the list $\{1, \ldots, n-1\}$ are quadratic residues. This follows from the fact that the equation

$$x^2 = v \mod n$$

for every $v \in \{1, \ldots, n-1\}$ has either 2 solutions (in the case when v is a quadratic residue) or no solutions (if v is not a quadratic residue). Indeed, such an equation cannot have more than two different solutions (modulo a prime number n, a polynomial of degree 2 cannot have more than 2 roots); the same time, if x is a one root of this equation, then $-x$ is another one (x and $-x$ must be different if n is an odd prime number).

Exercise 1. Prove that -1 is a quadratic residue modulo a prime number $p > 2$, if $p = 4k + 1$ for some integer k (and is *not* a quadratic residue modulo p, if $p = 4k + 3$ for some integer k).

Exercise 2. Let $p > 2$ be a prime number, and $p = 4k + 3$ for some integer k. Then the mapping

$$x \mapsto x^2 \mod p$$

is a permutation (bijection) of the set of quadratic residues modulo p.

3 Pseudo-random generator of Blum–Blum–Shub.

Assume we have a (strong) one-way function $f : \{0,1\}^* \to \{0,1\}^*$ such that for every n the restriction of f on the inputs of length k,

$$f : \{0,1\}^k \to \{0,1\}^k$$

is a bijection (a permutation of $\{0,1\}^k$). Assume also that this function has a hard-core predicate h. Then we can use f and h to construct a pseudo-random generators. We can do it as follows: for a *seed* $x_0 \in \{0,1\}^k$ we compute the sequence of strings

$$x_1 = f(x_0),\ x_2 = f(x_1),\ \dots,\ x_n = f(x_{n-1})$$

and let

$$b_1 = h(x_1), \dots, b_n = h(x_n).$$

One can show that the defined mapping

$$x_0 \mapsto b_1 \dots b_n$$

is a pseudo-random generator (assuming that $n > k$ and $n \le \mathrm{poly}(k)$).

The construction of a pseudo-random generator BBS (proposed by Lenore Blum, Manuel Blum, and Michael Shub) employs a similar idea. Let $m = p \cdot q$ be a product of two prime numbers. In what follows we assume that p and q are congruent to 3 modulo 4. For a seed $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$ we let

$$x_1 = x_0^2 \mod m,\ x_2 = x_1^2 \mod m,\ \dots,\ x_n = x_{n-1}^2 \mod m$$

(we assume that each x_i is an integer number between 1 and $n-1$). We define b_i (for $i = 1, \dots, n$) as the least significant bit of x_i. The constructed function

$$x_0 \mapsto b_1 \dots b_n$$

(for $n = \mathrm{poly}(\log k)$) is believed to be a pseudo-random generator. (To prove this hypothesis, we need to prove that the problem of integer factorisation is computationally hard.)

Remark 1. If p and q are are congruent to 3 modulo 4, then the mapping

$$x \mapsto x^2 \mod (pq)$$

is a bijection on the set o quadratic residues modulo $p \cdot q$. An efficient algorithm for inversion of this mapping would imply an efficient algorithm for the problem of integer factorisation of n of the form $n = p \cdot q$ (for p and q as defined above).

4 Cryptographic Hash functions

In the class we defined the notion of a *collision resistant* family of cryptographic hash functions. We discussed an application cryptographic hash functions to the scheme of electronic signature.

5 Zero Knowledge proofs

In the class we discussed a protocol of *zero knowledge proof* for the problem of 3-colorability of a graph and its cryptographic interpretation: *Prover* can convince *Verifier* that Prover knows a “secret password” (3-coloring of the given graph) without divulging any information on this coloring.